UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/772,256	01/29/2001	Hilarie K. Orman	1909.2.75A	9279

21186 7590 10/06/2005

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
1600 TCF TOWER
121 SOUTH EIGHT STREET
MINNEAPOLIS, MN 55402

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 10/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/772,256	ORMAN, HILARIE K.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-37 are pending.

2. Applicant was correct in noting that the previous office action mailed 12 July 2005 was incorrectly stated to be a final rejection. The instant office action repeats the same rejections as the prior office action and thus is a final rejection.

Response to Arguments

3. Applicant's arguments with respect to claims 1-37 have been considered but are not persuasive.

4. Applicant has argued on pages 8-11 that Claim 34 meets the requirements of 35 USC 101. Examiner respectfully disagrees. Applicant initially asserts that claim 34 is statutory by citing MPEP 2106(a) which allows that "a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory." Examiner acknowledges that a computer program embodied on a computer-readable medium is statutory; however, Examiner asserts that claim 34 provides no such program; it is instead a signal. The claimed signal is an entity identifier (see Claim 34 lines 1-2) and not a program as Applicant asserts.

5. Further, even if one interprets a signal to be a program, the claimed signal fails to meet the requirements of 35 USC 101. As Applicant has correctly noted, the test with § 101 is whether the claim as a whole produces a useful concrete and tangible result. However, Applicant's assertion that claim 34 meets this test because it is directed towards producing an entity identifier is incorrect. Claim 34 does not provide any positively recited steps for the production of an entity identifier. Claim 34 instead provides a non-functional data structure that is "adapted to be" transformed into an entity identifier. Language such as "adapted to" does not require steps to be performed nor does it limit a claim to a particular structure (see MPEP 2106 II(c)). Thus, Examiner maintains that claim 34 fails to meet the requirements of 35 USC § 101 by not providing a useful, concrete, and tangible result.

6. Applicant has argued on page 11 that the Gressel reference (US Patent No. 6,311,272) fails to anticipate claim 34. Examiner respectfully disagrees. Applicant has focused upon the alleged lack of a secret value in the entity identifier. Examiner contends that the DES key is evidence of a secret value (Gressel, column 15 lines 22-37). Thus, Gressel teaches an entity identifier in the form of a secret value, entity name, and random number (Gressel, column 15 lines 22-37, DES Key (secret value), own ID (entity name), challenge (random number)).

7. Applicant has argued on pages 12-13 that the combination of the Hoke reference (US Patent No. 6,701,437) and the Shimbo reference (US Patent No. 6,092,191) is

improper because the two inventions are mutually exclusive. Examiner respectfully disagrees with this assertion. Initially, Examiner notes that Shimbo has only been relied upon to teach the feature of an entity identifier acting as an index into a data structure for acquiring cryptographic context information (Shimbo, column 18 line 60 – column 19 line 7). There is ample motivation for the combination in view of this additional feature in that it provides the advantage of allowing the looking up of a key corresponding to an entity for use in authentication (Shimbo, column 1 line 60 – column 2 line 8, column 18 line 60 – column 19 line 7). Further, Examiner notes that VPN traffic, as in the Hoke reference, operates in overtop existing network protocols to exchange data over a public network. A VPN would not interfere with another security scheme already in place. Instead, a VPN connection establishes a connection between two VPN end units and encapsulates the VPN packet within a standard Internet packet (Hoke, Figure 2). This standard packet is sent across the network and is subject to the same security protocols as any other packet. Thus, Examiner maintains that the combination is proper because the teachings of the two cited references are not incompatible.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claim 34 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 34 is directed towards a signal

representing a non-functional data structure that produces no useful, concrete, or tangible result.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claim 34 is rejected under 35 U.S.C. 102(e) as being anticipated by Gressel US Patent No. 6,311,272.

11. With regards to claim 34, Gressel teaches an entity identifier comprising an encoded version of an entity name, secret value, and a random number (Gressel, column 15 lines 23-37) and wherein the encoded version of the entity name, the secret value and the random number are adapted to be bitwise concatenated with one another (Gressel, column 15 lines 23-37, own ID, DES key, public key) to produce an intermediate value, the intermediate value is adapted to be hashed to acquire a hash result (Gressel, column 15 lines 23-37), the hash result is adapted to be bitwise concatenated with the random number to produce the entity identifier (Gressel, column 15 lines 23-37, concatenate DES key with hashed id, key, key).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-5, 8, 13, 15-21, 25, 27-30, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoke et al US Patent No. 6,701,437 in view of Bruce Schneier's Applied Cryptography and Shimbo et al US Patent No. 6,092,191. Hoke discloses a method for processing communications in a virtual private network.

14. With regards to claims 1, 13, 17, 25, 27, and 35, Hoke teaches the connecting of an originally-connected entity to an original endpoint (Hoke, column 8 lines 37-44, VPN and destination endstation, column 8 lines 52-65), the originally-connected entity having an entity name and cryptographic context information (Hoke, column 15 lines 24-30, IP address, Hoke, column 8 lines 37-44 "encrypts"), and the creation of an entity identifier (Hoke, column 15 lines 41-50). Hoke fails to teach the encoding of the entity name and the secret value such that by using the secret value, information necessary to access the cryptographic context information can be retrieved and the entity identifier acting as an index into a data structure for acquiring cryptographic context information. Schneier teaches the encoding of the entity name and the secret value such that by using the secret value, information necessary to access the cryptographic context information can be retrieved (Schneier, Page 568, Paragraph 1 and Kerberos Version 5 Messages 2-

Kerberos to client, $K_{c\text{-}tgs}$ accessed using secret key Kc, and Tc). Shimbo teaches entity identifier acting as an index into a data structure for acquiring cryptographic context information (Shimbo, column 18 line 60 – column 19 line 7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's method of encrypting an entity name and cryptographic information and Shimbo's index method with Hoke's virtual private network because it offers the advantage of allowing providing a credential that an entity may use to contact an endpoint in a secure manner that provides authentication (Schneier, Page 568 Paragraph 1) and the advantage of allowing the looking up of a key corresponding to an entity for use in authentication (Shimbo, column 1 line 60 – column 2 line 8, column 18 line 60 – column 19 line 7).

15. With regards to claims 2 and 18, Hoke as modified teaches the passing of the entity identifier to at least one subsequently connecting computing entity that seeks to connect to the original endpoint (Schneier, Page 568, Paragraph 1 and Kerberos Version 5 Messages 2- Kerberos to client).

16. With regards to claims 3-4, 19 and 21, Hoke as modified teaches the decoding of the entity identifier using the secret key value, thereby determining information necessary to access cryptographic context information (Schneier, Page 568, Paragraph 1 and Kerberos Version 5 Messages 2- Kerberos to client, $K_{c\text{-}tgs}$ accessed using secret key Kc, and Tc).

17. With regards to claims 5, Hoke as modified teaches that there is at least one other trusted computing entity (Schneier, Page 567 Figure 24.1 TGS), the trusted

computing entity possessing a trusted entity name and the decoding step comprises encoding at least one trusted computer entity name and the secret value to produce a computed identifier and then comparing the computed identifier to the entity identifier to determine if they match (Schneier, Page 568, Tc contains server name, Page 570 section "Requesting a Service").

18. With regards to claim 8, Hoke as modified teaches the subsequently connecting entity using the originally-connected entity name to access the originally connected entity cryptographic context information and the subsequently connecting computing entity uses the originally connected entity cryptographic context information in a secure connection to the original endpoint (Schneier, Page 570 section "Requesting a Service").

19. With regards to claim 15, Hoke as modified teaches the encrypting algorithm being triple DES (Schneier, Pages 294-295).

20. With regards to claims 16 and 20, Hoke as modified teaches the originally connected endpoint being no longer connected to the original endpoint (Hoke, Figure 3, "End" Item 370).

21. With regards to claims 28-30, Hoke as modified teaches the encryption algorithm comprising symmetric key encryption, public key, or Diffie-Hellman key exchange encryption (Schneier, Page 568, "Credentials", encryption using secret key and Page 513, Diffie-Hellman).

22. Claims 6, 9-12, 14, 22-24, 26, 31-33, and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoke et al US Patent No. 6,701,437, Bruce Schneier's Applied Cryptography and Shimbo et al US Patent No. 6,092,191, as applied to claim 1 above, and further in view of Demers et al US Patent No. 5,857,023.

23. With regards to claims 6 and 22-24, Hoke as modified teaches all that is described above, but fails to teach the deconcatenating of a random number from the entity identifier prior to the decoding step. Demers teaches the deconcatenating of a random number from the entity identifier prior to the decoding step (Demers, column 9 lines 1-21). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Demer's deconcatenating step with Hoke as modified because it offers the advantage of providing an irrefutable method of reassuring a receiving party that the message came from a trusted entity (Demers, column 9 lines 1-11).

24. With regards to claims 9-10, 14, 26, 31-33 and 36-37, Hoke as modified fails to disclose the creating step comprising using a hash function with an input and an output comprising a bitwise concatenation of the entity name, the secret value, and a random number and the output of the hash function being at least bitwise concatenated with the random number. Demers teaches a creating step comprising using a hash function with an input and an output comprising a bitwise concatenation of the entity name, the secret value, and a random number and the output of the hash function being at least bitwise concatenated with the random number (Demers, column 8 line 62 – column 9 line 11). At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to utilize Demers' creating step with Hoke as modified because it offers the advantage of providing an irrefutable method of reassuring a receiving party that the message came from a trusted entity (Demers, column 9 lines 1-11).

25. With regards to claims 11-12, Hoke as modified teaches the use of SHA-1 and the hash function being invertible (Schneier, Page 442, "computationally infeasible to recover a message corresponding to a given message digest").

Conclusion

26. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100